

Generative AI: It's magic but fraught with legal risks

6 June 2023 6 min read

and Hlonelwa Lutuli, Candidate Attorney

The use and beneficial application of generative AI in the workplace is increasing at an exponential rate – with many businesses actively developing and adapting AI or AI being used organically within businesses without clear guidelines for use being in place.

While no AI-specific law or regulation has been passed in South Africa as yet, navigating the significant legal risks which AI adoption poses has become crucial. Key legal considerations should be front of mind for effectively and uniformly managing both the use of, and development of, generative AI tools within a business:

- **Confidentiality risks:**

- Information entered into prompts on generative AI systems will not remain confidential and may be shared with third parties for review purposes. Generative AI may use the data provided by a user to train and improve its AI model. For example, one of the ways in which OpenAI improves ChatGPT is by training the AI on the conversations people have with it (unless users opt out of permitting the use of their data for such AI training purposes or to improve their models or where the enterprise API is used (where a user has to specifically opt-in to share data)). Consequently, exposing business or third party confidential or proprietary information in prompts may breach contractual or statutory confidentiality obligations and compromise company trade secrets.

- **Data Protection considerations:**

- The inputting of and reuse, access to, sharing and further processing of identifiable personal information in AI systems could result in processing identifiable personal information that could fall foul of the [Protection of Personal Information Act of 2013](#).
- Data entered into prompts may be transferred across borders (including in the case of OpenAI whose servers are based outside of South Africa) where such transfers are subject to specific limitations in terms of data protection law.
- More stringent legislative rules generally apply to the processing of sensitive or special personal information, such as health data and biometric data (e.g. as used in facial recognition technology) and any collection, use and sharing of such information should be evaluated to address any privacy risks.
- The use of algorithms which undertake automated decision-making tasks should also be interrogated to ensure compliance with data protection laws.

- **Competition law considerations:**

- Accidentally or deliberately accessing company business information, trade secrets, confidential information or other competitively sensitive information of competitors using generative AI or sharing your own business information on a public AI platform could have anti-competitive implications as this information could be used to predict competitor behaviour or to adjust or co-ordinate pricing so as to enable competitors to indirectly or directly participate in price fixing or collusive tendering. Even if some form of price fixing or collusive tendering does not occur, possession and awareness of a competitor's competitively sensitive information is, in certain circumstances, regarded by the

Competition Commission as a contravention of the Competition Act 89 of 1998 or as indicative of an underlying anti-competitive arrangement.

- **Intellectual Property:**

- The use of generated content from generative AI may constitute copyright infringement in terms of the Copyright Act of 1978 on two grounds: (i) where the training datasets that the generative AI tool has been fed or trained on includes copyrighted works that neither the generative AI owner nor the user have a licence to use; or (ii) the generative AI tool produces responses or generates works that are similar to existing and protected works or replicates an existing work that is protected under copyright or other intellectual property laws.
- In respect of the intellectual property rights in new works created by using AI, the Copyright Act may vest authorship of the AI-generated content in either the user who inputs the prompt or the creator of the AI-tool. Even though the Open AI terms of use specifically assign intellectual property rights in generated content to the user, companies should consider appropriate mechanisms to address the risk that works generated by their employees' using generative AI tools may not vest in the company. Businesses may not be able to enforce intellectual property rights against third party use of such generated works.

- **Exposing proprietary source code on generative AI systems or using generative AI to develop proprietary code:**

- A company's proprietary computer code which is made accessible to a generative AI system could be exposed to the public and result in infringement of its intellectual property rights. Significant security risks may also result from the exposure of the source code on an AI system. Another consideration is that such code may be subsumed into open source software.
- Where a company uses generative AI to develop computer code, the new work may be based on a third party's intellectual property rights where third party proprietary code is incorporated into the generated result. Such generated code may not meet compliance and/or industry standards for mitigating against vulnerabilities in such code and meeting minimum security standards.

- **Incorrect or discriminatory information:**

- As generative AI is trained on data which may contain incorrect information or reflect biases or offensive content, there is a risk that the AI tool outputs may be false and/or could be considered discriminatory or offensive. Distribution of such content within the workplace may have implications under the Employment Equity Act and Labour Relations Act. The distribution of incorrect or offensive or discriminatory content outside of the business could give rise to potential civil and delictual liability.

- **Reputational risk:**

- A company's inability to avoid or mitigate against the legal risks highlighted above has the residual impact of causing lasting damage to the organisation's reputation. The basis of this lies in the fact that a failure to mitigate against these risks may leave a company's business partners, clients and trade secrets at risk. Further, with the boom of AI-detection software in the market, companies may also need to consider the reputational risk of using content that can easily be identified as AI-generated without labelling the content as such.

Interesting Read – [Raging against the machine](#)

Innovation and digitalisation strategies of many businesses increasingly place reliance on AI tools and not incorporating some form of generative AI tools into a business' operations may hinder the business' competitive edge against competitors who are effectively and successfully using AI to optimise their operations. Therefore, the key to successfully managing AI risk and navigating any legal and reputational risks lies in the adoption of appropriate rules and policy guidelines for the consistent and responsible use of AI within a company's operations, including by implementing appropriate internal measures to mitigate against such risks.



Preeta Bhagattjee

Head of Technology & Innovation

[View Profile](#)